# TAMPER-RESISTANT PACKAGING AND APPROACH

The present invention is directed to device packaging and, more particularly, to tamper-resistant packaging for items such as integrated circuits.

Packaging plays an important role in product protection and security. For instance, in electronics and software applications, packaging is important for ensuring that products are kept free from damage and are not tampered with. Tamper-prevention has been particularly important in applications where information stored within a particular package is proprietary. For example, in memory applications, it is sometimes desirable to prevent access to data stored in a circuit.

A variety of approaches to protecting stored data have been used. For example, in SRAM applications, memory is lost when power is removed from the circuitry used to store data. Power is removed when tampering is detected, thus erasing the stored data. When these approaches involve battery backup, the battery power is also removed in response to tampering.

In other memory applications, power is not necessarily required for storing data. For example, in magnetic memory applications, memory is stored in a manner that does not require power to maintain the memory and thus is non-volatile. Certain types of magnetic memory cells that use the magnetic state of a region for altering the electrical resistance of materials located near the region are collectively known as magnetoresistive (MR) memory cells. An array of magnetic memory cells is often called a magnetic random access memory (MRAM). In MRAM applications, memory cells are typically formed on intersections of word lines and sense lines, with each memory cell typically having magnetic layers separated by a conductive or insulating layer. Magnetoresistive metals used in such memory applications show a change in electrical resistance when placed in a magnetic field. In this regard, the MRAM cell has two stable magnetic configurations, one having high resistance and the other low resistance (*e.g.*, with high resistance representing a logic state zero and low resistance representing a logic state one). The magnetic state (*i.e.*, magnetic charge) of the device is manipulated and read as data, such that the read can be effected using an instrument to probe an integrated circuit on which the MRAM cell is located.

Protecting memory in applications relying on power to maintain memory, as well as those applications that do not necessarily require power to maintain memory (*i.e.*, non-volatile memory), has been challenging. In particular, protecting non-volatile memory has been challenging because typical approaches involving power-related tamper protection do

not work. Specifically, removing power does not cause memory loss. In addition, techniques previously used for protecting both non-volatile and volatile memory from probing tend to rely upon the detection of a probe via a disturbance in clock stream or a sudden increase in load capacitance. When non-conducting and/or non-contacting probing techniques are used, previously-available probe detection techniques have limited effect. These and other difficulties present challenges to the implementation of tamper-protection and packaging for a variety of applications.

Various aspects of the present invention involve tamper protection for a variety of integrated circuits, such as memory circuits and others. The present invention is exemplified in a number of implementations and applications, some of which are summarized below.

According to one example embodiment, an integrated circuit arrangement includes an integrated circuit device, which has a plurality of magnetically-responsive circuit nodes. The integrated circuit arrangement also comprises a package including a plurality of magnetized particles, where the package is adapted to inhibit access to the integrated circuit device. The magnetically-responsive circuit nodes magnetically respond to the plurality of magnetized particles such that a change in the magnetic field collectively provided by the magnetized particles renders a change in a magnetic state of at least one of the magnetically-responsive circuit nodes.

According to another example embodiment, an integrated circuit arrangement comprises an integrated circuit chip and a plurality of magnetically-responsive memory elements which are adapted to store a logical state as a function of a magnetic state of a magnetic element which applies a magnetic field to the magnetically-responsive memory element. The integrated circuit arrangement further comprises a package covering at least a portion of the integrated circuit chip and which prevents access to the portion of the integrated circuit chip. The package also includes a plurality of magnetic particles where at least some of the plurality of magnetically-responsive memory elements have a logic state that is responsive to a magnetic field generated by at least one of the plurality of magnetic particles. Also included in the integrated circuit arrangement is a tamper-protection circuit which is adapted to detect the logic state of at least some of the plurality of magnetically-responsive memory elements and in response to detecting a logic state changing, to detect that the package has been tampered with.

The above summary of the present invention is not intended to describe each embodiment or every implementation of the present invention. The above summary of the present invention is not intended to describe each illustrated embodiment or every implementation of the present invention. The figures and detailed description that follow more particularly exemplify these embodiments.

The invention may be more completely understood in consideration of the following detailed description of various embodiments of the invention in connection with the accompanying drawings, in which:

FIG. 1 is an integrated circuit arrangement including a package and integrated circuit device arranged for inhibiting the tampering of circuitry in the device, according to an example embodiment of the present invention; and

FIG. 2 is a flow diagram for a tamper protection approach, according to another example embodiment of the present invention.

While the invention is amenable to various modifications and alternative forms, specifics thereof have been shown by way of example in the drawings and will be described in detail. It should be understood, however, that the intention is not to limit the invention to the particular embodiments described. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the scope of the invention as defined by the appended claims.

The present invention is believed to be applicable to a variety of circuits and approaches involving and/or benefiting from tamper protection, and in particular to the detection of tampering of a packaged integrated circuit without necessarily relying upon power or interruption and/or the detection of an electrical characteristic. While the present invention is not necessarily limited to such applications, an appreciation of various aspects of the invention is best gained through a discussion of examples in such an environment.

According to an example embodiment of the present invention, a tamper-protection arrangement includes a package arranged to cover at least a portion of an integrated circuit chip where the chip contains at least one magnetically-responsive element. The package is also arranged to prevent access to at least a portion of the integrated circuit chip. The package includes a plurality of magnetic particles which are arranged to cause a detectable magnetic response in at least one magnetically-responsive element. The tamper-protection arrangement further includes a tamper-protection circuit which is adapted to detect the magnetic response of at least one magnetically-responsive element and to detect a change in

the magnetic field provided by the magnetic particles. Such a change could be the result of various events some examples being: a probe being positioned near the package, the existence of another magnetic field near the package, or the removal or partial removal of the package from the arrangement. Such a change in the magnetic field would indicate that the circuit arrangement was tampered with.

FIG. 1 shows an integrated circuit device 100 having a substrate 104 having circuitry 108 therein and further covered by a package 106 adapted for inhibiting tampering, according to another example embodiment of the present invention. The substrate 104 includes circuitry 108 and a plurality of magnetically-responsive circuit elements 130-134 (*e.g.*, MRAM elements, magnetic junction transistors or magnetic tunnel junction elements). The package 106 has magnetic particles 120-125 in various portions thereof, with at least some of the magnetic particles arranged to cause one or more of the magnetically-responsive circuit elements 130-134 to take on a magnetic state (*e.g.*, a polarization direction). For example, the magnetic particle 124 causes the magnetically-responsive circuit element 133 to take on a selected magnetic state.

With the package 106 in place, the state of at least some of the plurality of magnetically-responsive circuit elements 130-134 is detected and stored as a reference that represents an untampered condition. During operation (*e.g.*, during power-up) of the integrated circuit device 100, the stored reference is compared with real-time states of the magnetically-responsive circuit elements 130-134. If a portion of the package 106 including a magnetic particle has been tampered with (*e.g.*, removed), the real-time state of one or more of the magnetically-responsive circuit elements 130-134 is correspondingly altered. For instance, referring again to magnetically-responsive circuit element 133, when a portion of the package 106 including the magnetic particle 124 is removed, the state of the magnetically-responsive element 133 is no longer influenced by the magnetic particle 124. Without the influence of the magnetic particle 124, the magnetically-responsive element 133 is free to take on a state relative to other magnetic fields present. With this approach, access to the circuitry 108 for probing, visual inspection and/or other purposes is detected.

In a further example embodiment, the integrated circuit device 100 includes a tamper-detection circuit 160 adapted to detect and respond to tampering detected as a function of the state of one or more of the magnetically-responsive circuit elements 130-134. In one implementation, the tamper-detection circuit includes a memory adapted to store data representative of an untampered state of the magnetically-responsive circuit

elements 130-134. During subsequent operation of the integrated circuit device 100, a real-time state of the magnetically-responsive circuit elements 130-134 is detected and compared at the tamper-detection circuit 160 with the stored untampered state. If the real-time detected state matches the stored untampered state, a condition representing no tampering is detected. However, if the real-time detected state does not match the stored untampered state, a tamper condition is detected as the change in position and/or removal of one or more of the magnetic particles 120-125.

In another implementation, the tamper-detection circuit 160 is adapted to respond to a tamper condition by altering a characteristic of the integrated circuit device 100. For instance, when the circuitry 108 includes memory, the tamper-detection circuit 160 is adapted to erase some or all of the memory. In another instance, the tamper-detection circuit is adapted to set a flag representing the detection of tampering. The flag can then be detected by another user, for instance, upon visual or electronic detection, either locally with the integrated circuit device 100 or remotely, such as via the Internet (*e.g.*, wherein the integrated circuit device 100 is connected to the Internet).

Referring now to FIG. 2, one particular approach to tamper-detection involves storing a reference signal representative of a logical state of selected magnetically-responsive memory cells and using the reference signal as a comparison, according to another example embodiment of the present invention. At block 210, a package is formed over an integrated circuit device having magnetically-responsive memory cells therein. The package includes a plurality of magnets, with the magnets arranged to affect the logical state of some of the magnetically-responsive memory cells. After the package is in place, the state of at least some of the magnetically-responsive memory cells is detected at block 220. The state is stored as a reference in a memory, such as a one-time programmable ROM, at block 230.

During operation of the integrated circuit chip, the state of the magnetically-responsive memory cells is detected at block 240. At block 250, the state detected at block 240 is compared with the reference state detected at block 220 and stored at block 230. When the states match at block 260, a condition of no tampering is detected at block 270. When the states do not match at block 260, a tamper condition is detected at block 280. In further implementations, the tamper condition detected at block 280 is used to effect a response to the tampering, such as by erasing memory or setting a tamper-detection flag.

The various embodiments described above and shown in the figures are provided by way of illustration only and should not be construed to limit the invention. Based on the above discussion and illustrations, those skilled in the art will readily recognize that various modifications and changes may be made to the present invention without strictly following the exemplary embodiments and applications illustrated and described herein. Such modifications and changes do not depart from the true spirit and scope of the present invention that is set forth in the following claims.